PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-312477
(43)Date of publication of application : 09.11.2001

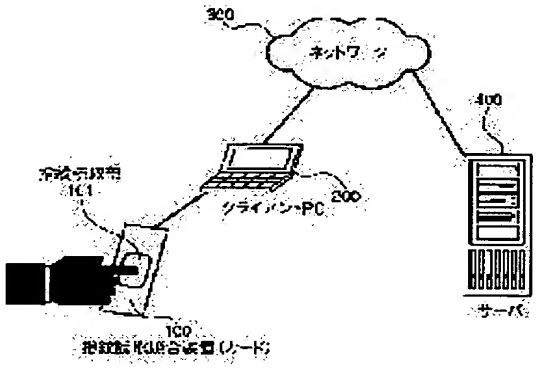
(51)Int.Cl. G06F 15/00
G09C 1/00
H04L 9/32

(21)Application number : 2000-131674
(22)Date of filing : 28.04.2000

(71)Applicant : NIPPON YUNISHISU KK
SYSTEM NEEDS KK
(72)Inventor : YATSUKAWA NAONOBU
NAKAYAMA KEISUKE

(54) SYSTEM, DEVICE, AND METHOD FOR AUTHENTICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To solve the problem such that the possibility of 'impersonation' can not be denied as to an existent authentication system even when authentica tion is successful at the time of remote access through a network, i.e., an authen ticator is unable to prove that a person who is operating a personal computer of a client as an authenticated person is a legal user.
SOLUTION: A remote authenticating program with high security using code is built in an intelligent portable device 100 having a function of inputting and matching biological features of an authenticated person inside and in the device 100 which are hardly accessed from outside, local authentication by biological feature authentication and high-security remote authentication are combined. Consequently, the genuiness of the user obtained by a client PC 200 is transmitted to a remote authentication server 400 to actualize remote individual authentication.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－312477
（P2001－312477A）
(43)公開日　平成13年11月９日(2001.11.9)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ　５Ｂ０８５
			３３０Ｇ　５Ｊ１０４
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｅ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ
			６７３Ｅ

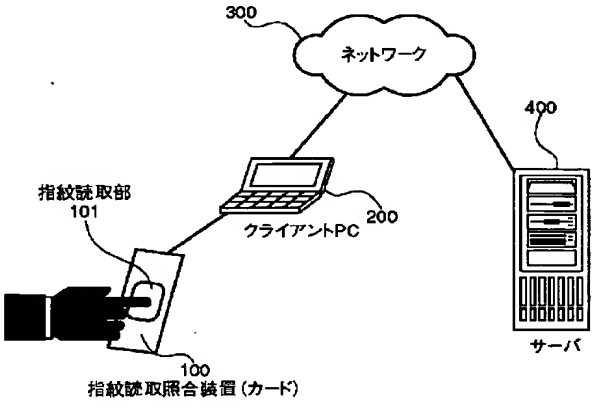
審査請求　未請求　請求項の数８　ＯＬ　（全　６　頁）　最終頁に続く

(21)出願番号　特願2000－131674(P2000－131674)
(22)出願日　平成12年４月28日(2000.4.28)

(71)出願人　591030237
日本ユニシス株式会社
東京都港区赤坂２丁目17番51号
(71)出願人　597115082
システムニーズ株式会社
東京都港区芝大門２丁目12番９号
(72)発明者　八津川　直伸
東京都港区赤坂二丁目17番51号　日本ユニシス株式会社内
(72)発明者　中山　恵介
東京都港区芝浦４－９－21
(74)代理人　100076428
弁理士　大塚　康徳　（外１名）
最終頁に続く

(54)【発明の名称】　認証システム、並びに、認証装置およびその方法

(57)【要約】
【課題】　ネットワークを介したリモートアクセス時の認証が成功しても、既存の認証方式では「成り済まし」の可能性は否定できない。つまり、認証者は、被認証者であるクライアントのパーソナルコンピュータを操作している人間が正当な利用者本人であるか否かの確証を得ることができない。
【解決手段】　被認証者の生体特徴を入力し照合する機能を内蔵するインテリジェントな可搬型デバイス100内に、暗号を利用した高セキュリティなリモート認証処理プログラムを内蔵させ、外部からのアクセスが極めて困難なデバイス100内で生体特徴認証によるローカル認証と高セキュリティなリモート認証を連結させる。これによって、クライアントPC200で得られた利用者の真正性を遠隔の認証サーバ400へ伝播させ、遠隔個人認証を実現する。



1

【特許請求の範囲】
【請求項１】　被認証者の生体的な特徴を入力し照合するローカル認証を行うローカル認証手段、および、暗号を利用した高セキュリティなリモート認証手段を有する可搬型のデバイスを利用して、ネットワークを介した遠隔認証を行う認証システムであって、
前記リモート認証手段は、前記ローカル認証が成功した場合、前記遠隔認証に必要な認証情報を生成し、
前記遠隔認証を行う認証装置は、前記ネットワークを介して送られてくる認証情報に基づき、前記ローカル認証により前記被認証者の真正性が確認されたことを認識することを特徴とする認証システム。
【請求項２】　ネットワークを介したリモートアクセスにおける利用者を認証する認証装置であって、
前記利用者に関する生体的な特徴を示す情報が記録された記録手段と、
前記利用者の生体的な特徴を示す情報を入力する入力手段と、
前記入力手段により入力された生体的な特徴を示す情報と、前記記録手段に記録された生体的な特徴を示す情報とを照合する照合手段と、
前記照合手段の照合結果に応じて、前記リモートアクセスに必要な認証情報を生成する生成手段とを有することを特徴とする認証装置。
【請求項３】　前記生成手段は、前記照合が一致する場合に前記認証情報を生成することを特徴とする請求項2に記載された認証装置。
【請求項４】　前記生成手段は、種情報および秘密鍵を用いた暗号処理により前記認証情報を生成することを特徴とする請求項2または請求項3に記載された認証装置。
【請求項５】　さらに、前記生成手段によって生成される認証情報を、前記ネットワークを介してリモート認証を行う他の認証装置へ送るために出力する出力手段を有することを特徴とする請求項2から請求項4の何れかに記載された認証装置。
【請求項６】　前記認証装置はカード形状を有することを特徴とする請求項2から請求項5の何れかに記載された認証装置。
【請求項７】　ネットワークを介したリモートアクセスにおける利用者を認証する認証方法であって、
前記利用者の生体的な特徴を示す情報を入力し、
メモリから前記利用者に関する生体的な特徴を示す情報を読み出し、
前記入力手段により入力された生体的な特徴を示す情報と、前記メモリから読み出された生体的な特徴を示す情報とを照合し、
その照合結果に応じて、前記リモートアクセスに必要な認証情報を生成することを特徴とする認証方法。
【請求項８】　ネットワークを介したリモートアクセスにおける利用者を認証する認証装置に使用される記憶媒体であって、

2

前記利用者に関する生体的な特徴を示す特徴情報と、
前記特徴情報と、入力手段により入力される生体的な特徴を示す情報とを照合するプログラムコードと、
その照合結果に応じて、前記リモートアクセスに必要な認証情報を生成するプログラムコードとを有することを特徴とする記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は認識システム、並びに、認証装置およびその方法に関し、例えば、ネットワークを介したリモートアクセスにおける利用者個人を認証する認証システム、並びに、認証装置およびその方法に関する。
【０００２】
【従来の技術】ネットワークを介して遠隔地にあるコンピュータにアクセスする利用者の認証の方法には、ユーザIDとパスワードとを組み合わせた所謂パスワード認証方式、および、パスワード認証方式のセキュリティ向上を図ったワンタイムパスワード認証方式がある。
【０００３】パスワード認証方式は、パスワードを推測したり、通信中のパスワードを盗聴することで、容易に第三者が利用者に「成り済ます」ことが可能である。
【０００４】ワンタイムパスワード認証方式には、チャレンジレスポンス方式や携帯型のワンタイムパスワード発生器を利用するものがある。
【０００５】チャレンジレスポンス方式では、認証者側のコンピュータが「チャレンジ」と呼ばれる毎回異なるデータを被認証者側のコンピュータへ送信する。チャレンジを受信した被認証者は、予め認証者と共有し秘密に保持するパスワードとチャレンジとをある一方向性関数に通し、その出力を一回限り有効な認証用パスワードとして認証者側のコンピュータに返す。
【０００６】携帯型のワンタイムパスワード発生器を利用した方式では、通常、利用者がこの発生器を保持し、これにより発生されるパスワードと、予め認証者と共有し秘密に保持するPIN(Personal Identification Number)とを組み合わせた文字列を一回限り有効なパスワードとして認証者側のコンピュータに送信する。
【０００７】これらワンタイムパスワード認証方式は、パスワード認証方式の欠点の一つであるパスワードの盗聴による「成り済まし」は不可能である。
【０００８】しかし、チャレンジレスポンス認証方式における上記のパスワードや、ワンタイム認証方式における上記のPINは、利用者である被認証者自身が記憶（保持）すべき情報であり、その意味では、パスワード認証方式のセキュリティ強度と同等でしかない。すなわち、利用者が覚えやすい文字列や数字列を使用すれば、第三者に容易に見破られたり推測されたりする。また、セキュリティを考慮して無意味の文字列や数字列を使用する

場合もあるが、言い換えれば覚え難い文字列や数字列になるので、その備忘録としてそれを何処かへメモすれば、逆にセキュリティを低下させることになる。

【０００９】また、被認証者側のコンピュータが盗まれる、あるいは、そのコンピュータを第三者が無断使用して認証に成功してしまえば、認証者側は、相手が正当な利用者でないにもかかわらずアクセスを許可してしまう。

【００１０】さらに、特開平11-282982号には、盗難の危険が少ない、持ち運び可能なICカードと暗号とを用いた認証方法が開示されている。しかし、ICカードの真正な所持者を特定するためにパスワード入力を必要とする点からすれば、そのセキュリティ強度はパスワード認証方式と同じである。

【００１１】

【発明が解決しようとする課題】認証処理を行う実態（認証者）は、認証対象である相手方のパーソナルコンピュータ(PC)を操作する人間、すなわち本来認証されるべき実態（被認証者）が認証者の管理するサーバにアクセスする際、通常は、パスワード方式、チャレンジレスポンス方式あるいはワンタイムパスワード方式など種々の認証手段を用いて被認証者の正当性を確認し、第三者による「成り済まし」を排除する。

【００１２】パスワードなどの情報は、現実には、被認証者のPCなどのハードウェアやソフトウェアから送られてくる。このため、認証者からみれば、被認証者を認証すべき瞬間に、被認証者がサーバの正当な利用者であるか否かを確認することができない。これは、上述したように、PCが盗まれる、PCを第三者が無断使用する、上記のICカードを利用する認証方法の場合はICカードを紛失した、盗まれた、あるいは、パスワードやPINが漏洩する、推測されるなどがあり得るからである。

【００１３】本発明は、上述の問題を解決するためのものであり、ネットワークを介したリモートアクセスにおける利用者を認証することを目的とする。

【００１４】また、認証におけるパスワードやPINなどを不要にすることを他の目的とする。

【００１５】さらに、認証情報を生成するのに必要な情報を、認証者と被認証者との間で通信する必要がない認証を行うことを他の目的とする。

【００１６】

【課題を解決するための手段】本発明は、前記の目的を達成する一手段として、以下の構成を備える。

【００１７】本発明にかかる認証システムは、被認証者の生体的な特徴を入力し照合するローカル認証を行うローカル認証手段、および、暗号を利用した高セキュリティなリモート認証手段を有する可搬型のデバイスを利用して、ネットワークを介した遠隔認証を行う認証システムであって、前記リモート認証手段は、前記ローカル認証が成功した場合、前記遠隔認証に必要な認証情報を生成し、前記遠隔認証を行う認証装置は、前記ネットワークを介して送られてくる認証情報に基づき、前記ローカル認証により前記被認証者の真正性が確認されたことを認識することを特徴とする。

【００１８】本発明にかかる認証装置は、ネットワークを介したリモートアクセスにおける利用者を認証する認証装置であって、前記利用者に関する生体的な特徴を示す情報が記録された記録手段と、前記利用者の生体的な特徴を示す情報を入力する入力手段と、前記入力手段により入力された生体的な特徴を示す情報と、前記記録手段に記録された生体的な特徴を示す情報とを照合する照合手段と、前記照合手段の照合結果に応じて、前記リモートアクセスに必要な認証情報を生成する生成手段とを有することを特徴とする。

【００１９】本発明にかかる認証方法は、ネットワークを介したリモートアクセスにおける利用者を認証する認証方法であって、前記利用者の生体的な特徴を示す情報を入力し、メモリから前記利用者に関する生体的な特徴を示す情報を読み出し、前記入力手段により入力された生体的な特徴を示す情報と、前記メモリから読み出された生体的な特徴を示す情報とを照合し、その照合結果に応じて、前記リモートアクセスに必要な認証情報を生成することを特徴とする。

【００２０】

【発明の実施の形態】以下、本発明の一実施例として、可搬性に優れたインテリジェントな生体特徴入力照合デバイスと暗号アルゴリズムとを利用した認証方式を、図面を参照して説明する。

【００２１】生体の特徴を入力し照合するデバイスの例として、出願人は、特開平10-336169号に記載した無限ワンタイム認証方式が実装された薄型・軽量のカード型指紋読取照合装置（以降「カード」と呼ぶ）がある。このカードには、所持者である被認証者の指紋情報およびワンタイム性を有する一回限り有効な認証子（以降「認証子」と呼ぶ）を生成するための暗号鍵が予め登録されている。この暗号鍵は、公開鍵暗号方式においては秘密鍵、共通鍵暗号方式においては共通鍵に相当するが、本実施形態の説明における暗号鍵は秘密鍵である。

【００２２】カードの所持者である被認証者は、目的のサーバにアクセスする際、カードをPCに接続して、カードに自身の指紋を読み取らせる。そして、読み取らせた指紋と、指紋カードに登録済みの指紋情報または指紋特徴点（テンプレート）データとを照合させる。すなわち、カードが、カード所持者を認証し、カードの所持者の正当性を確認する。このような認証を「ローカル認証」と呼ぶことにする。

【００２３】ローカル認証が成功すると、カードに実装されている暗号処理プログラムが、カード内に保存されている暗号鍵（秘密鍵）を使用して認証子を生成し、それをPCおよび通信路経由で目的のサーバに送信する。勿

論、指紋情報、テンプレートおよび暗号鍵そのものが送信されることはないから、通信路上におけるプライバシや情報の漏洩を防ぐことができる。

【００２４】認証子を受信したサーバは、前述の秘密鍵と対をなす公開鍵および暗号処理プログラムにより、認証子の正当性を検証、すなわち被認証者の認証を行う。このような認証を「リモート認証」と呼ぶことにする。

【００２５】リモート認証が成功すると、被認証者のPCは目的のサーバにアクセス可能になり、目的のサーバ上の各種アプリケーションやリソースを使用することが可能になる。勿論、認証が失敗すれば、認証者は、サーバと被認証者のPCとの間の通信路を遮断する。

【００２６】このように生体の特徴を利用したローカル認証と、暗号を利用した強力なリモート認証を、外部からのアクセスを遮断した耐タンパ（tamper、改竄）性を有するデバイスであるカード内で連結させる仕組みにより、ローカル認証で得られた本人の真正性を認証者に安全に伝播させることが可能になる。

【００２７】次に、図1を参照して、クライアントPC200がネットワーク300を経由して目的のサーバ400にアクセスする場合を説明する。この際のリモート認証方式としては、前述したように、公開鍵暗号方式を基礎とする無限ワンタイム認証方式を採用する。また、生体特徴照合デバイスには、前述した薄型・軽量の可搬性に優れたカード型指紋読取照合デバイス（カード）100を採用する。

【００２８】図2は、クライアントPC200と、それに接続されたカード100内にそれぞれ実装されるソフトウェアモジュールの構成例を示す図である。また、図3はローカル認証およびリモート認証の一連の流れを示すシーケンス図である。

【００２９】利用者が所持するカード100の内部には、ローカル認証に必要なカード所持者の指紋情報106、指紋照合プログラム105、リモート認証に必要なワンタイム性を有する認証子を生成するための種データ(S)103、暗号処理プログラム104、および、暗号化に必要な秘密鍵(Ks)102が格納されている。

【００３０】ユーザからリモートアクセスが要求されると(S1)、クライアントPC200上の認証処理プログラム110は、ユーザに対してカード100の指紋読取部101によって指紋を入力するよう促す(S2)。

【００３１】指紋情報が入力されると(S3)、カード100の指紋照合処理プログラム105は、入力された指紋情報と、カード100の所持者の指紋情報である指紋情報106とを比較してローカル認証を行う(S4)。そして、両情報が不一致であれば、その旨のメッセージを認証処理プログラム110に返して、リモートアクセス要求を拒絶する(S5)。一方、両情報が一致すれば、暗号処理プログラム104により、無限ワンタイム認証方式によるリモート認証のための認証子が、種データ(S)103および秘密鍵(Ks)102から生成される(S6)。

【００３２】ここで、指紋照合がカード100内の指紋照合プログラム105で行われることが極めて重要である。すなわち、ユーザの指紋情報はカード100の外部へ流出することはなく、指紋情報106の偽造による「成り済まし」は不可能である。従って、真正なユーザしかカード100は使用できず、カード100を紛失したり、盗まれた場合でも、カード100が不正アクセスに利用されることはない。さらに、ユーザのプライバシも保護することができるから、生体情報（指紋）を認証に用いることに対するユーザの心理的抵抗は少ないと考えられる。

【００３３】また、認証子の生成が、すべてカード100内の暗号処理プログラム104によって行われることも重要である。すなわち、秘密鍵(Ks)102についてのいかなる情報もカード100の外部へ流出することはなく、出力されるのは認証子のみである。無限ワンタイム認証方式によれば、生成される認証子は毎回異なるから、たとえ認証子が盗聴されたとしても再利用は不可能で、かつ、秘密鍵(Ks)102が得られなければ認証子を偽造することもできない。

【００３４】カード100内で生成された認証子はクライアントPC200へ送られ(S7)、さらに通信路を経て目的のサーバ400へ送られる(S8)。そして、サーバ400は、無限ワンタイム認証方式によるリモート認証を行い(S9)、認証結果をクライアントPC200に返す(S10)。認証が成功すればクライアントPC200と目的のサーバ400との間でデータの送受信が開始される(S11)。また、認証に失敗した場合は、サーバ400は直ちに通信路を遮断する(S12)。

【００３５】このように、リモート認証のための認証子を生成するには、カード100内に保存されている秘密鍵(Ks)102が必要である。そして、この秘密鍵(Ks)102を使用できるのは、ローカル認証に成功した正当なカード所持者だけである。従って、認証者は、リモート認証が成功した時点で、クライアントPC200を操作している人間が、サーバ400の正当な利用者であることの確証を得たことになる。言い換えると、遠隔地に存在する個人の認証（遠隔個人認証）が実現されたことになる。

【００３６】

【変形例】上述した実施形態は、その趣旨を逸脱しない範囲で種々の変形が可能である。

【００３７】上記では、ローカル認証のための認証情報としてユーザの生体特徴である指紋を用いる例を説明したが、指紋以外の生体特徴情報も利用することが可能である。例えば、網膜パターン、虹彩、掌形、耳の形、顔のパターン、顔の温度分布および音声スペクトルなどである。それらを測定（入力）および照合する機能、アクセス制御可能なデータ記憶管理機能および暗号処理プログラムが格納されたデバイスであれば、上記の実施形態と同様の遠隔個人認証が可能になる。

【００３８】また、一種類の生体特徴だけでなく、二種

類以上の生体特徴を測定（入力）および照合するデバイスであれば、ローカル認証のセキュリティをより向上させることができる。

【００３９】また、生体特徴入力照合デバイスとして、極薄ICカードタイプ、携帯電話内蔵型、ゲーム機内蔵型および腕時計内蔵型などが考えられる。凡そ、個人が身に付けたり、持ち歩いたりする物品にバイオデバイスを内蔵すれば、ネットワークを介したリモートアクセスにおいて、認証者に対して、何時でも利用者の真正性が簡単に証明することができる。

【００４０】上記では、リモート認証方式として無限ワンタイム認証方式を利用する例を説明したが、セキュリティ強度が強固、すなわち盗聴やリプレイ攻撃に耐え得る方式であれば他の認証方式を採用しても構わない。例えば、共通鍵による多値暗号文を発生させることが可能なカオス多値暗号方式を利用して認証する方式が挙げられる。この場合、認証子の生成には種データを使用する方法とチャレンジレスポンス認証方式を利用する方法がある。

【００４１】このように、本実施形態によれば、ネットワークを介した認証処理において、コンピュータを使用してアクセスしてきた相手が正当なアクセス権を有する人間か否かを、遠隔であるにもかかわらず、厳密に認証することができる。その際、被認証者個人の生体特徴情報（指紋など）は、本人が所持する生体特徴入力照合デバイスに登録されているだけであり、認証者側（遠隔の認証サーバ）には一切登録する必要がないし、生体特徴入力照合デバイスと認証サーバとの間で生体特徴情報がやり取りされることもない。従って、このような認証システムの利用者の心理的抵抗感を排除することができ、かつ、認証サーバの運用も容易になる。

【００４２】

【発明の効果】以上説明したように、本発明によれば、ネットワークを介したリモートアクセスにおける利用者を認証することができる。

【００４３】また、認証におけるパスワードやPINなどを不要にすることができる。

【００４４】さらに、認証情報を生成するのに必要な情報を、認証者と被認証者との間で通信する必要がない認証を行うことができる。

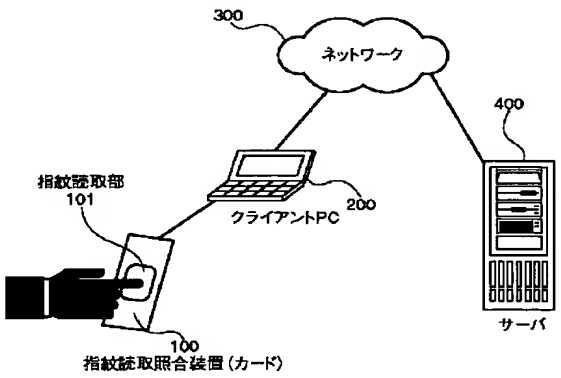
【図面の簡単な説明】

【図１】生体検知型遠隔個人認証システムの構成例を示す図、

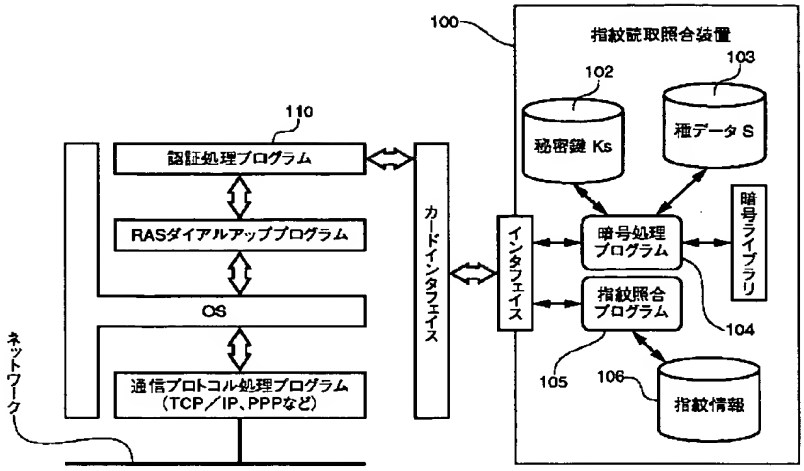
【図２】生体検知型遠隔個人認証システムにおけるクライアント側のソフトウェアモジュールの構成例を示す図、

【図３】認証処理の流れを示すシーケンス図である。

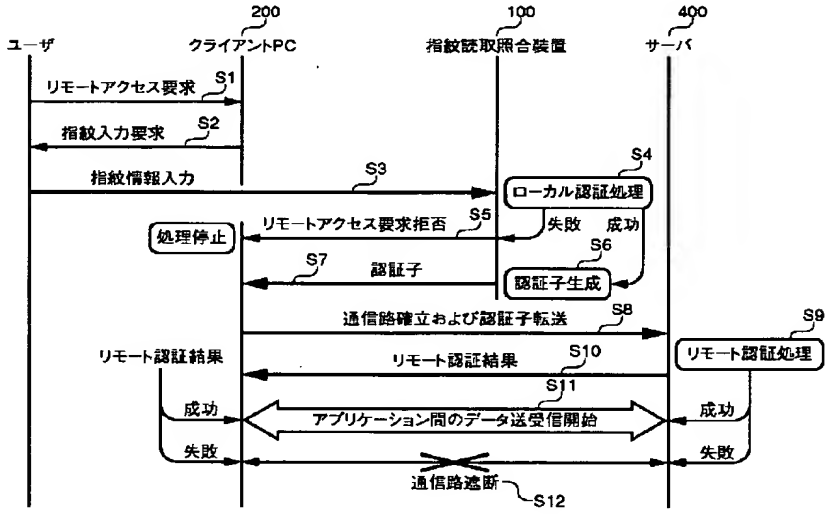
【図１】



【図２】



【図３】



フロントページの続き

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ(参考)
		Ｈ０４Ｌ　9/00	６７３Ａ

Ｆターム(参考)　5B085 AA08 AE12 AE15 AE23 AE25
AE26 AE29 BG07
5J104 AA07 KA01 KA04 KA06 KA17
NA02 NA35 NA37 NA38 NA40
NA42 PA07